Amendments to the Specification

Please replace the paragraph at page 5, lines 6-15, with the following amended paragraph:

In the above-mentioned public-key cryptosystem, for example, an RSA cryptosystem, its public key measures 10-fold and more as long as the presently used telephone number, thus being very troublesome. To guard against this, in the ID-NIKS, each ID information can be registered in a form of name list to thereby be referenced in generating a common key used between any given entities. Therefore, by safely implementing such an ~~IK-NIKS~~ ID-NIKS system as shown in FIG.1, a convenient cryptosystem can be installed over a computer network to which a lot of entities are subscribed. For these reasons, the ID-NIKS is expected to constitute a core of the future cryptosystem.

Please replace the paragraph at page 16, lines 14-17, with the following amended paragraph:

Next, safety according to the present invention will be described. The safety of the present invention is based on an elliptic curve discrete logarithm problem and an extended elliptic curve discrete logarithm problem equivalent thereto as will be described below.

Please replace the paragraph at page 20, lines 17-21, with the following amended paragraph:

However, it is necessary to solve the following extended elliptic curve discrete logarithm problem to obtain the coefficient u_i in the equation (15). Accordingly, such an attack is hard to perform. Consequently, the safety is based on the difficulty of the solution of the extended elliptic discrete logarithm problem.

Please replace the paragraph at page 23, lines 7-13, with the following amended paragraph:

If V_j and r_{ij} are given, it is apparent that u_i can be solved. Accordingly, the problem for solving the above equation (15) is equivalent to the extended elliptic discrete logarithm problem. Moreover, if a group of elliptic curves is ~~periodic~~ cyclic, it is apparent that the extended elliptic discrete logarithm problem is equivalent to the elliptic discrete logarithm problem. In this case, accordingly, the problem for solving the above equation (15) is equivalent to the elliptic discrete logarithm problem.

Please replace the first three lines of equations following line 8 of page 24 with the following amended equations:

$$\begin{aligned}K_{ac} &= \langle S_a, P_c \rangle \\ &= \langle S_a, u_1P_1 + u_2P_2 + \cdots + u_nP_n \rangle \\ &= \langle S_a, P_1 \rangle^{u_1} \langle S_a, P_2 \rangle^{u_2} \cdots \langle S_a, P_n \rangle^{u_n}\end{aligned}$$

Please replace the two lines of equations on page 27, immediately preceding the paragraph beginning with "Moreover, the entity...", with the following amended equations:

$$= \prod_{j=1}^{n} \left\langle \sum_{i=1}^{n} r_{ij} P_{ai}, P_{bj} \right\rangle$$

$$= \prod_{j=1}^{n} \prod_{i=1}^{n} \langle P_{ai}, P_{bj} \rangle^{r_{ij}} \cdots (30)$$

Please replace the equation following page 28, line 12, with the following amended equation:

$$K_{ab} = \prod_{j=1}^{n} \prod_{i=1}^{n} \langle P_{ai,} P_{bj} \rangle^{r_{ij}} \cdots (31)$$